THAT WHICH IS CLAIMED:

Sub B2

1. A method of controlling updates of a programmable memory of a device, the method comprising:

obtaining an update image corresponding to the update of the programmable memory;

obtaining a certificate associated with the update image, the certificate having update application rules in at least one extension of the certificate;

extracting the update application rules from the at least one extension of the obtained certificate; and

selectively updating the programmable memory based on the update image and the update application rules extracted from the obtained certificate.

2. A method according to Claim 1, wherein the update application rules comprise at least one of rules information associated with a manufacturer of the device, rules information associated with a brand of the device, rules information associated with a software version of the device, rules information associated with a license authorization of the device or rules associated with the individual device.

3. A method according to Claim 1, wherein the update application rules comprise rules defining devices for which application of the update image is authorized.

4. A method according to Claim 3, wherein the rules defining devices comprise rules specifying at

least one of authorized device serial numbers, authorized firmware versions, authorized device manufacturers and authorized users associated with a device.

5. A method according to Claim 1, wherein the update application rules comprise rules defining how data from the update image is utilized to update the programmable memory.

6. A method according to Claim 1, wherein the update application rules comprise rules which identify installation information provided with the update image and wherein the step of updating the programmable memory comprises updating the programmable memory utilizing the installation information provided with the update image.

7. A method according to Claim 6, wherein the installation information comprises an install program and wherein the step of updating the programmable memory utilizing the installation information comprises executing the install program to write the update data to the programmable memory.

8. A method according to Claim 1, further comprising verifying the authenticity of the update image.

9. A method according to Claim 8, wherein the step of verifying the authenticity of the update

comprises the step of evaluating the certificate associated with the update image to determine if a valid digital signature is provided with the image.

10. A method according to Claim 8, wherein the step of verifying the authenticity of the update image comprises the step of determining if a valid digital signature is provided with the image by decrypting the digital signature provided with the image using a shared secret.

11. A method according to Claim 9, wherein the step of evaluating the certificate comprises the steps of:

decrypting a digital signature of the certificate utilizing a public key of a certificate authority accessible to the update program; and

comparing the decrypted digital signature with a precomputed value to determine if the digital signature is a valid digital signature associated with the certificate authority.

12. A method according to Claim 11, wherein the public key is stored in a non-updateable memory.

13. A method according to Claim 11, further comprising the steps of:

providing the public key of the certificate authority in a previous version of data to be stored in the programmable memory; and

wherein the step of decrypting a digital signature of the certificate utilizing a public key further comprises the step of obtaining the public key from the programmable memory.

14. A method according to Claim 8, wherein the update image includes a plurality of certificates in a hierarchy of certificates and wherein the step of verifying the authenticity of the update comprises the step of evaluating certificates of the plurality of certificates in the update image to determine if a valid digital signature is provided with the certificates of the update image.

15. A method according to Claim 14, wherein the step of evaluating each of the digital certificates comprises the steps of:

decrypting a digital signature of a certificate utilizing a public key associated with a next-higher certificate in the hierarchy;

comparing the decrypted digital signature with a precomputed value to determine if the digital signature is a valid digital signature associated with the certificate;

obtaining a public key associated with another of the digital certificates;

repeating the steps of decrypting and comparing utilizing the obtained public key associated with another of the digital certificates; and

wherein the step of obtaining a public key is repeated until a public key associated with a digital

certificate of a trusted certificate authority is obtained, and comparing the of the trusted certificate authority public key with a predetermined value.

16. A method according to Claim 1, wherein the update image includes a plurality of certificates in a hierarchy of certificates and wherein the extracting the update application rules comprises the step of extracting update application rules from each of the certificates in the hierarchy of certificates having update application rules provided in an extension of the certification.

17. A method according to Claim 16, wherein the programmable memory is updated with the update image only if all of the update application rules indicate that the update image is applicable to the device.

18. A method according to Claim 16, wherein the programmable memory is updated with the update image if any of the update application rules indicate that the update image is applicable to the device.

19. A method according to Claim 1, wherein the programmable memory is updated with the update image if any of the update application rules indicate that the update image is applicable to the device.

20. A method according to Claim 1, wherein the programmable memory is updated with the update image

only if all of the update application rules indicate that the update image is applicable to the device.

21. A system for controlling updates of a programmable memory of a device, comprising:

means for obtaining an update image corresponding to the update of the programmable memory;

means for obtaining a certificate associated with the update image, the certificate having update application rules in at least one extension of the certificate;

means for extracting the update application rules from the at least one extension of the obtained certificate; and

means for selectively updating the programmable memory based on the update image and the update application rules extracted from the obtained certificate.

22. A system according to Claim 21, wherein the update application rules comprise at least one of rules information associated with a manufacturer of the device, rules information associated with a brand of the device, rules information associated with a software version of the device, rules information associated with a license authorization of the device or rules associated with the individual device.

23. A system according to Claim 21, wherein the update application rules comprise rules defining

devices for which application of the update image is authorized.

24. A system according to Claim 23, wherein the rules defining devices comprise rules specifying at least one of authorized device serial numbers, authorized firmware versions, authorized device manufacturers and authorized users associated with a device.

25. A system according to Claim 21, wherein the update application rules comprise rules defining how data from the update image is utilized to update the programmable memory.

26. A system according to Claim 21, wherein the update application rules comprise rules which identify installation information provided with the update image and wherein the means for updating the programmable memory comprises means for updating the programmable memory utilizing the installation information provided with the update image.

27. A system according to Claim 26, wherein the installation information comprises an install program and wherein means for updating the programmable memory utilizing the installation information comprises means for executing the install program to write the update data to the programmable memory.

28. A system according to Claim 21, further comprising means for verifying the authenticity of the update image.

29. A system according to Claim 28, wherein the means for verifying the authenticity of the update comprises means for evaluating the certificate associated with the update image to determine if a valid digital signature is provided with the image.

30. A system according to Claim 28, wherein the means for verifying the authenticity of the update image comprises means for determining if a valid digital signature is provided with the image by decrypting the digital signature provided with the image using a shared secret.

31. A system according to Claim 29, wherein the means for evaluating the certificate comprises:

means for decrypting a digital signature of the certificate utilizing a public key of a certificate authority accessible to the update program; and

means for comparing the decrypted digital signature with a precomputed value to determine if the digital signature is a valid digital signature associated with the certificate authority.

32. A system according to Claim 31, wherein the public key is stored in a non-updateable memory.

33. A system according to Claim 31, further comprising:

means for providing the public key of the certificate authority in a previous version of data to be stored in the programmable memory; and

wherein the means for decrypting a digital signature of the certificate utilizing a public key further comprises means for obtaining the public key from the programmable memory.

34. A system according to Claim 28, wherein the update image includes a plurality of certificates in a hierarchy of certificates and wherein the means for verifying the authenticity of the update comprises means for evaluating certificates of the plurality of certificates in the update image to determine if a valid digital signature is provided with evaluated certificates of the update image.

35. A system according to Claim 34, wherein the means for evaluating each of the digital certificates comprises:

means for decrypting a digital signature of a certificate utilizing a public key associated with a next-higher certificate in the hierarchy;

means for comparing the decrypted digital signature with a precomputed value to determine if the digital signature is a valid digital signature associated with the certificate;

means for obtaining a public key associated with another of the digital certificates;

means for repeatedly obtaining a public key, decrypting a digital signature and comparing the decrypted digital signature with a precomputed value until a public key associated with a digital certificate of a trusted certificate authority is obtained; and

means for comparing the public key of the digital certificate of the trusted certificate authority with a predetermined value.

36. A system according to Claim 21, wherein the update image includes a plurality of certificates in a hierarchy of certificates and wherein the means for extracting the update application rules comprises means for extracting update application rules from each of the certificates in the hierarchy of certificates having update application rules provided in an extension of the certification.

37. A system according to Claim 36, wherein the programmable memory is updated with the update image only if all of the update application rules indicate that the update image is applicable to the device.

38. A system according to Claim 36, wherein the programmable memory is updated with the update image if any of the update application rules indicate that the update image is applicable to the device.

39. A system according to Claim 21, wherein the programmable memory is updated with the update image if

any of the update application rules indicate that the update image is applicable to the device.

40. A system according to Claim 21, wherein the programmable memory is updated with the update image only if all of the update application rules indicate that the update image is applicable to the device.

41. A computer program product for controlling updates of a programmable memory of a device, comprising:

a computer readable media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which obtains an update image corresponding to the update of the programmable memory;

computer readable program code which obtains a certificate associated with the update image, the certificate having update application rules in at least one extension of the certificate;

computer readable program code which extracts the update application rules from the at least one extension of the obtained certificate; and

computer readable program code which selectively updates the programmable memory based on the update image and the update application rules extracted from the obtained certificate.

42. A computer program product according to Claim 41, wherein the update application rules comprise at

least one of rules information associated with a manufacturer of the device, rules information associated with a brand of the device, rules information associated with a software version of the device, rules information associated with a license authorization of the device or rules associated with the individual device.

43. A computer program product according to Claim 41, wherein the update application rules comprise rules defining devices for which application of the update image is authorized.

44. A computer program product according to Claim 43, wherein the rules defining devices comprise rules specifying at least one of authorized device serial numbers, authorized firmware versions, authorized device manufacturers and authorized users associated with a device.

45. A computer program product according to Claim 41, wherein the update application rules comprise rules defining how data from the update image is utilized to update the programmable memory.

46. A computer program product according to Claim 41, wherein the update application rules comprise rules which identify installation information provided with the update image and wherein the computer readable program code which updates the programmable memory

comprises computer readable program code which updates the programmable memory utilizing the installation information provided with the update image.

47. A computer program product according to Claim 46, wherein the installation information comprises an install program and wherein the computer readable program code which updates the programmable memory utilizing the installation information comprises computer readable program code which executes the install program to write the update data to the programmable memory.

48. A computer program product according to Claim 41, further comprising computer readable program code which verifies the authenticity of the update image.

49. A computer program product according to Claim 48, wherein the computer readable program code which verifies the authenticity of the update comprises computer readable program code which evaluates the certificate associated with the update image to determine if a valid digital signature is provided with the image.

50. A computer program product according to Claim 48, wherein the computer readable program code which verifies the authenticity of the update image comprises computer readable program code which determines if a valid digital signature is provided with the image by

decrypting the digital signature provided with the image using a shared secret.

51. A computer program product according to Claim 49, wherein the computer readable program code which evaluates the certificate comprises:

computer readable program code which decrypts a digital signature of the certificate utilizing a public key of a certificate authority accessible to the update program; and

computer readable program code which compares the decrypted digital signature with a precomputed value to determine if the digital signature is a valid digital signature associated with the certificate authority.

52. A computer program product according to Claim 51, wherein the public key is stored in a non-updateable memory.

53. A computer program product according to Claim 51, further comprising:

computer readable program code which provides the public key of the certificate authority in a previous version of data to be stored in the programmable memory; and

wherein the computer readable program code which decrypts a digital signature of the certificate utilizing a public key further comprises computer readable program code which obtains the public key from the programmable memory.

54. A computer program product according to Claim 48, wherein the update image includes a plurality of certificates in a hierarchy of certificates and wherein the computer readable program code which verifies the authenticity of the update comprises computer readable program code which evaluates certificates of the plurality of certificates in the update image to determine if a valid digital signature is provided with the evaluated certificates of the update image.

55. A computer program product according to Claim 54, wherein the computer readable program code which evaluates each of the digital certificates comprises:

computer readable program code which decrypts a digital signature of a certificate utilizing a public key associated with a next-higher certificate in the hierarchy;

computer readable program code which compares the decrypted digital signature with a precomputed value to determine if the digital signature is a valid digital signature associated with the certificate;

computer readable program code which obtains a public key associated with another of the digital certificates;

computer readable program code which repeatedly obtains a public key, decrypts a digital signature and compares the decrypted digital signature with a precomputed value until a public key associated with a digital certificate of a trusted certificate authority is obtained; and

computer readable program code which compares the public key of the digital certificate of the trusted certificate authority with a predetermined value.

56. A computer program product according to Claim 41, wherein the update image includes a plurality of certificates in a hierarchy of certificates and wherein the computer readable program code which extracts the update application rules comprises computer readable program code which extracts update application rules from each of the certificates in the hierarchy of certificates having update application rules provided in an extension of the certification.

57. A computer program product according to Claim 56, wherein the programmable memory is updated with the update image only if all of the update application rules indicate that the update image is applicable to the device.

58. A computer program product according to Claim 56, wherein the programmable memory is updated with the update image if any of the update application rules indicate that the update image is applicable to the device.

59. A computer program product according to Claim 41, wherein the programmable memory is updated with the update image if any of the update application rules indicate that the update image is applicable to the device.

60. A computer program product according to Claim 41, wherein the programmable memory is updated with the update image only if all of the update application rules indicate that the update image is applicable to the device.

61. A certificate for use in updating a programmable memory, the certificate comprising:

a digital signature; and

at least one extension having rules to control installation of an update image.

62. A certificate according to Claim 61, wherein the certificate is signed with a private key of a certificate authority.

63. A certificate according to Claim 61, wherein the certificate is a certificate in a hierarchy of a plurality of certificates.

64. A certificate according to Claim 63, wherein the certificate is signed with a private key of a next-higher authority associated with a next-higher certificate in the hierarch of certificates.

65. A certificate according to Claim 61, wherein the rules comprise at least one of rules information associated with a manufacturer of the device, rules information associated with a brand of the device, rules information associated with a software version of

the device, rules information associated with a license authorization of the device or rules associated with the individual device.

66. A certificate according to Claim 61, wherein the rules comprise rules defining devices for which application of the update image is authorized.

67. A certificate according to Claim 66, wherein the rules defining devices comprise rules specifying at least one of authorized device serial numbers, authorized firmware versions, authorized device manufacturers and authorized users associated with a device.

68. A ~~method~~ certificate according to Claim 61, wherein the rules comprise rules defining how data from the update image is utilized to update the programmable memory.

69. A method of providing a plurality of devices having differing functionality, the method comprising:

providing a plurality of generic processing devices having hardware suitable to perform at least a portion of the differing functionality of the plurality of devices, wherein the generic processing devices also have a programmable memory;

distributing to the plurality of generic processing devices updates to the programmable memory so as to define the functionality of the generic processing devices so as to provide the plurality of devices having differing functionality, wherein the

updates have at least one associated certificate, the certificate having update application rules in at least one extension of the certificate; and

selectively updating the programmable memories of the generic processing devices based on the distributed updates and the rules specified in the at least one extension of the certificate.

70. A method according to Claim 69, wherein the step of distributing to the plurality of generic processing devices comprises the step of transmitting updates of the programmable memory over the Internet.

71. A method according to Claim 70, wherein the plurality of generic processing devices comprise automobiles and wherein the updates of the programmable memory to control options provided for the automobiles.

72. A method of providing a plurality having differing functionality, the method comprising:

distributing through a non-secure distribution channel a plurality of devices; and

controlling the functionality of individual ones of the plurality of devices by a secure update of the individual ones of the plurality of devices, wherein the update is controlled by a trusted update authority within the distribution channel.

73. A method according to Claim 72, wherein the secure update comprises transmitting update information over the Internet.

74. A method according to Claim 72, wherein the plurality of processing devices comprise automobiles and wherein the secure updates comprise updates of a programmable memory of the automobiles to control options provided with the automobiles.